



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/017,438	12/05/2001	Neil Y. Iwamoto	36.P325	6310
5514	7590	04/11/2006	EXAMINER	
FITZPATRICK CELLA HARPER & SCINTO 30 ROCKEFELLER PLAZA NEW YORK, NY 10112			VU, THONG H	
			ART UNIT	PAPER NUMBER
			2142	

DATE MAILED: 04/11/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/017,438	IWAMOTO ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Thong H. Vu	2142	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 17 November 2005.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-16 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-16 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

1. Claims 1-16 are pending. Claims 1,11-13,15 have been amended by Amendment filed on 8/31/2005.
2. According the Telephone communication on 4/06/06 with Michael K. O'Neil, attorney of applicant, the previous Office Action is vacated. The new Non- Final is follow.

### ***Claim Objections***

3. Claim 14 is objected to under 37 CFR 1.75(c) as being in improper form because a multiple dependent claim 1-10. See MPEP § 608.01(n). Accordingly, the claim 14 has not been further treated on the merits.

Claim 14 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. Claim 14 perform a method according to any (?) of claims 1-10. Appropriate correction is required.

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-7,9-16 are rejected under 35 U.S.C. 102(e) as being anticipated by Horen et al [Horen 2002/0049846 A1].

4. As per claim 1, Horen discloses A method for controlling access to a networked peripheral device by a user, wherein the networked peripheral device (i.e.: disk drive, CD-ROM, 0027) is accessible by both the user based on centralized access management information (i.e.: server) [Horen, server, 0020] the method comprising:

receiving access management information for the user at the networked peripheral device from a centralized location [Horen, distributing the quota across multiple file system, 0026];

determining, at the networked peripheral device, a feature and /or service provided by the networked peripheral device and a usage quota which restricts the user's use of the feature and /or service, based on the received access management information [Horen, restricts by policy, determine the resource quota, 0026];

allowing the user to access the to the networked peripheral device based on the determined feature and /or service and the determined\_usage quota corresponding to the feature and /or service [Horen, the resource quota is determined based on attributes and values, 0030].

5. As per claim 2, Horen discloses the networked peripheral device is a multifunction peripheral device as inherent features of network devices.

6. As per claim 3, Horen discloses the access management information is supplied by an authentication server once the authentication server authenticates the user based on authentication information received from the networked peripheral device [Horen, authorization, authentication, 0042].

7. As per claim 4, Horen discloses a user interface is devised by the networked peripheral device that is specific to the determined feature and /or service and corresponding quota [Horen, asset group based on quota, 0026].

8. As per claim 5, Horen discloses on a keypad on the device are enabled and/or disabled according to the determined feature and /or service and corresponding quota [Horen, asset group based on quota, 0026].

9. As per claim 6, Horen discloses the user is walk-up user, and wherein the access management information is supplied by an authentication server that authenticates both the walk-up user and the remote user [Horen, Internet ,WAN, 0019].

10. As per claim 7, Horen discloses the authentication information is a username and/or password [Horen, authorization, authentication, 0042].

11. As per claim 9, Horen discloses the access management information is encrypted [Horen, encoder, 0029].

12. As per claim 10, Horen discloses the authentication information received from the networked peripheral device is encrypted [Horen, encoder, 0029].

13. Claims 11-13,15 contain the similar limitations as set forth in claim 1. Therefore, claims 11-13,15 are rejected for the same rationale set forth in claim 1.

14. As per claim 14, Horen discloses network peripheral device is accessible by the user based on centralized access management information, said computer-executable process steps comprising process steps executable to perform a method according to any of claims 1 to 10 [see rejection claims 1-7 and 9-10].

15. As per claim 16, Horen discloses the server retrieves authentication information for the user from a directory service [Horen, file directory, subdirectories, 0020].

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Horen et al [Horen 2002/0049846 A1] in view of Auger [6,115,696]

16. As per claim 8, Horen discloses a computer system serving multiple users including the network peripheral device such as disk drive, CD-ROM [Horen, 0027]. However Horen does not explicitly detail "the authentication information is entered by inserting a **smart card** at the networked peripheral device".

In the same endeavor, Auger discloses a network management and distribution orders issued by user-clients using a smart card [Auger, col 2 line 36] access from a peripheral unit [Auger, col 5 lines 23-34] based on a quota [Auger, col 6 line 17-20]

Therefore it would have been obvious to an ordinary skill in the art at the time the invention was made to incorporate the technique of accessing the peripheral devices by a smart card based on the quota as taught by Auger into the Horen's apparatus in order to utilize the management of administration software. Doing so would provide efficiently and systematically managing the network transaction.

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

17. Claims 1-16 are rejected under 35 U.S.C. § 103 as being unpatentable over Greene et al [Greene, 6,782,396 B2] in view of Gree et al [Greer, 5,969,316].

18. As per claim 1, Greene discloses A method for controlling access to a networked peripheral device by a user, wherein the networked peripheral device is accessible by both the user based on centralized access management information [Greene, server, network and peripheral devices, Fig 1, col 2 lines 23-col 3 line 25], the method comprising:

receiving access management information for the user at the networked peripheral device from a centralized location [Greene, server, network, peripheral devices, Fig 1, col 2 line 23-col 3 line 25];

receiving access management information for the user at the networked peripheral device from a centralized location [Greene, learning and teaching styles, col 5 lines 20-35 et seq.];

determining, at the networked peripheral device, a feature and /or service provided by the networked peripheral device and a usage quota which restricts the user's use of the feature and /or service, based on the received access management information; and the determined usage quota corresponding to the feature and /or service [Greene, the quota and restriction, col 7 lines 14-59; the format of lesson is based on the learning style being tested, col 6 lines 15-23];

Greene also taught the data processing system includes PDA, kiosk, notebook computer or Web appliance [Greene, col 4 lines 26-32]. However Greene does not detail

“allowing the user to access the to the networked peripheral device based on the determined feature and /or service “



In the same endeavor, Greer discloses the smart card with a preconfigured data included a quota and authorize or allow a user to purchase at terminal devices [Greer, col 2 line 25-col 3 line 30]

Therefore it would have been obvious to an ordinary skill in the art at the time the invention was made to incorporate the technique of accessing the terminal devices by a smart card based on the quota and privileges of users as taught by Greer into the Greene's apparatus in order to utilize the management of administration software. Doing so would provide efficiently and systematically managing the learning capabilities with teaching capabilities.

19. As per claim 2, Greene-Greer disclose the networked peripheral device is a multifunction peripheral device as inherent features of peripheral devices.

20. As per claim 3, Greene-Greer disclose the access management information is supplied by an authentication server once the authentication server authenticates the user based on authentication information received from the networked peripheral device [Greer, authorized users, col 3 lines 1-17].

21. As per claim 4, Greene-Greer disclose a user interface is devised by the networked peripheral device that is specific to the determined function and corresponding quota [Greene, the quota and restriction, col 7 lines 14-59; the format of lesson is based on the learning style being tested, col 6 lines 15-23].

22. As per claim 5, Greene-Greer disclose on a keypad on the device are enabled and/or disabled according to the determined function and corresponding quota [Greene, the quota and restriction, col 7 lines 14-59; the format of lesson is based on the learning style being tested, col 6 lines 15-23].

23. As per claim 6, Greene-Greer disclose the user is walk-up user, and wherein the access management information is supplied by an authentication server that authenticates both the walk-up user and the remote user [Greer, smart card and network of vending operations, col 3 lines 17- 30].

24. As per claim 7, Greene-Greer disclose the authentication information is a username and/or password [Greer, authorized users, col 3 lines 1-17].

25. As per claim 8, Greene-Greer disclose the authentication information is entered by inserting a smart card at the networked peripheral device [Greer, col 2 line 25-col 3 line 30].

26. As per claim 9, Greene -Greer disclose the access management information is encrypted [Greene, coded formats and decoded, col 8 lines 47-65].

27. As per claim 10, Greene -Greer disclose the authentication information received from the networked peripheral device is encrypted [Greene, coded formats and decoded, col 8 lines 47-65].

28. Claims 11-13,15 contain the similar limitations as set forth in claim 1. Therefore, claims 11-13,15 are rejected for the same rationale set forth in claim 1.

29. As per claim 14, Greene-Greer disclose network peripheral device is accessible by the user based on centralized access management information, said computer-executable process steps comprising process steps executable to perform a method according to any of claims 1 to 10 [see rejection claims 1-10].

30. As per claim 16, Greene-Greer disclose the server retrieves authentication information for the user from a directory service [Greene, database, col 4 lines 39-57].

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-16 are rejected under 35 U.S.C. 102(e) as being anticipated by Antonin et al [Antonin 2002/0032655 A1].

31. As per claim 1, Antonin discloses A method for controlling access to a networked peripheral device by a user [Antonin, PC based financial service kiosk, 0081], wherein the networked peripheral device is accessible by both the user based on centralized access management information [Antonin, 0037] the method comprising:

receiving access management information for the user at the networked peripheral device from a centralized location [Antonin, 0037];

determining, at the networked peripheral device, a feature and /or service provided by the networked peripheral device and a usage quota which restricts the user's use of the feature and /or service, based on the received access management information [Antonin,0042];

allowing the user to access the to the networked peripheral device based on the determined feature and /or service and the determined usage quota (i.e.: transaction amount) corresponding to the feature and /or service [Antonin, 0050,0051,0058].

32. As per claim 2, Antonin discloses the networked peripheral device is a multifunction peripheral device as inherent features of network devices.

33. As per claim 3, Antonin discloses the access management information is supplied by an authentication server once the authentication server authenticates the

Art Unit: 2142

user based on authentication information received from the networked peripheral device [Antonin, authorization, 0050; authentication, 0114].

34. As per claim 4, Antonin discloses a user interface is devised by the networked peripheral device that is specific to the determined feature and /or service and corresponding quota [Antonin, 0006,0051]

35. As per claim 5, Antonin discloses on a keypad on the device are enabled and/or disabled according to the determined feature and /or service and corresponding quota [Antonin, 0006,0051]

36. As per claim 6, Antonin discloses the user is walk-up user, and wherein the access management information is supplied by an authentication server that authenticates both the walk-up user and the remote user [Horen, Internet ,0122].

37. As per claim 7, Antonin discloses the authentication information is a username and/or password [Antonin, authorization, 0050; authentication, 0114].

38. As per claim 8, Antonin discloses the authentication information is entered by inserting a smart card at the networked peripheral device [Antonin, credit card, card reader, 0003].

39. As per claim 9, Antonin discloses the access management information is encrypted [Antonin, encryption, 0115].

40. As per claim 10, Antonin discloses the authentication information received from the networked peripheral device is encrypted [Antonin, encryption, 0115].

41. Claims 11-13,15 contain the similar limitations as set forth in claim 1. Therefore, claims 11-13,15 are rejected for the same rationale set forth in claim 1.

42. As per claim 14, Antonin discloses network peripheral device is accessible by the user based on centralized access management information, said computer-executable process steps comprising process steps executable to perform a method according to any of claims 1 to 10 [see rejection claims 1-7 and 9-10].

43. As per claim 16, Antonin discloses the server retrieves authentication information for the user from a directory service [Antonin, directors,0104].

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent

Art Unit: 2142

granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-14 are rejected under 35 U.S.C. 102(e) as anticipated by Bhogal

[7,010,607 B1].

44. As per claim 1, Bhogal discloses A method for controlling access to a networked peripheral device by a user, wherein the networked peripheral device is accessible by the user based on centralized access management information, the method comprising:

receiving access management information for the user at the networked peripheral device from a centralized location [Bhogal, server 104, printer 114 Fig 1]

determining, at the networked peripheral device, a feature and/or service provided by the networked peripheral device which the user can use and a usage quota which restricts the user's use of the feature and/or service based on the received access management information [Bhogal, print quotas, col 4 line 61-col 5 line 5]

allowing the user access to the networked peripheral device based on the determined feature and/or service and the determined usage quota corresponding to the feature and/or service [Bhogal, allowing the print job to print, col 5 lines 42-63].

45. As per claim 2 Bhogal discloses the networked peripheral device is a multifunction peripheral device as inherent feature of peripheral device.

46. As per claim 3, Bhogal discloses the access management information is supplied by an authentication server once the authentication server authenticates the user based

on authentication information received from the networked peripheral device [Bhogal, Internet, gateway, col 2 lines 48-58].

47. As per claim 4, Bhogal discloses a user interface is devised by the networked peripheral device that is specific to the determined feature and/or service and corresponding usage quota [Bhogal, print quotas, col 4 line 61-col 5 line 5].

48. As per claim 5, Bhogal discloses buttons on a keypad on the device are enabled and/or disabled according to the determined feature and/or service and corresponding usage quota [Bhogal, print quotas, col 4 line 61-col 5 line 5].

49. As per claim 6, Bhogal discloses the user is a walk-up user, and wherein the access management information is supplied by an authentication server that authenticates both the walk-up user and a remote user [Bhogal, Internet, gateway, col 2 lines 48-58].

50. As per claim 7, Bhogal discloses the authentication information is a username and/or password [Bhogal, Internet, gateway, col 2 lines 48-58].

51. As per claim 8, Bhogal discloses the authentication information is entered by inserting a smart card at the networked peripheral device as inherent feature of peripheral device.



52. As per claim 9, Bhogal discloses the access management information is encrypted (i.e.: proxy) [Bhogal, Internet, gateway as proxy node, col 2 lines 48-58].

53. As per claim 10, Bhogal discloses the authentication information received from the networked peripheral device is encrypted (i.e.: proxy) [Bhogal, Internet, gateway as proxy node, col 2 lines 48-58].

54. As per claim 11-13 contain the similar limitations set forth in claims 1-10. therefore claims 11-13 are rejected for the same rationale set forth in claims 1-10.

55. As per claim 14, Bhogal discloses Computer-executable process steps stored on a computer readable medium, said computer-executable process steps for controlling access to a networked peripheral device by a user, wherein the networked peripheral device is accessible by the user based on centralized access management information, said computer-executable process steps comprising process steps executable to perform a method according to any of Claims 1 to 10 [see rejection claim 1-10].

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 15-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bhogal et al [Bhogal, 7,010,607 B1] in view of Holt et al [Holt 6,070,192].

56. As per claim 15, Bhogal discloses A server for use in controlling access to a networked peripheral device by a user, wherein the networked peripheral device is accessible by the user based on centralized access management information, the server comprising a processor executing processing steps of:

receiving a request for access management information,  
transmitting access management information for the user indicating a feature and/or service provided by the networked peripheral device which the user can use and a usage quota the request including authentication information;

Bhogal also taught a gateway controls the access via Internet [Bhogal col 2 lines 48-58]. However Bhogal does not explicitly detail

authenticating the user using the authentication information; and a quotas which restricts the user's use of the feature and/or service in a case that authentication of the user is successful.

In the same endeavor, Holt discloses a control access transport service provides the call control and monitoring features including service quotas [Holt, col 13 lines 14-25] wherein a network access server and network gateways perform all AAA (Authentication, Authorization and Accounting) and once the user is authorized [Holt, col 11 lines 8-35]

Therefore it would have been obvious to an ordinary skill in the art at the time the invention was made to incorporate the authentication information and process as taught by Holt into the Bhogal's apparatus in order to utilize the monitoring process. Doing so would provide the Network gateway ability to direct data and handling bandwidth capability [Holt, col 2 liners 49-67].

57. As per claim 16, Bhogal-Holt disclose said server retrieves authentication information for the user from a directory service to detect the abnormal or absent state to the monitoring and detection system [Holt, a central directory, col 7 lines 34-59].

Any inquiry concerning this communication or earlier communications from the examiner should be directed to examiner *Thong Vu*, whose telephone number is (571)-272-3904. The examiner can normally be reached on Monday-Thursday from 6:00AM-3:30PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, *Andrew Caldwell*, can be reached at (571) 272-3868. The fax number for the organization where this application or proceeding is assigned is 571-273-8300

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PMR or Public PMR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

*Thong Vu*  
*Primary Examiner*  
*Art Unit 2142*

